2007

Security Primitives for Reconfigurable Hardware [presentation]

Huffmire, Ted

Ted Huffmire. Security Primitives for Reconfigurable Hardware. Faculty Candidate Seminar, Department of Computer Science, Room GE-117, Naval Postgraduate School, Monterey, CA,

FPGA SUMMIT

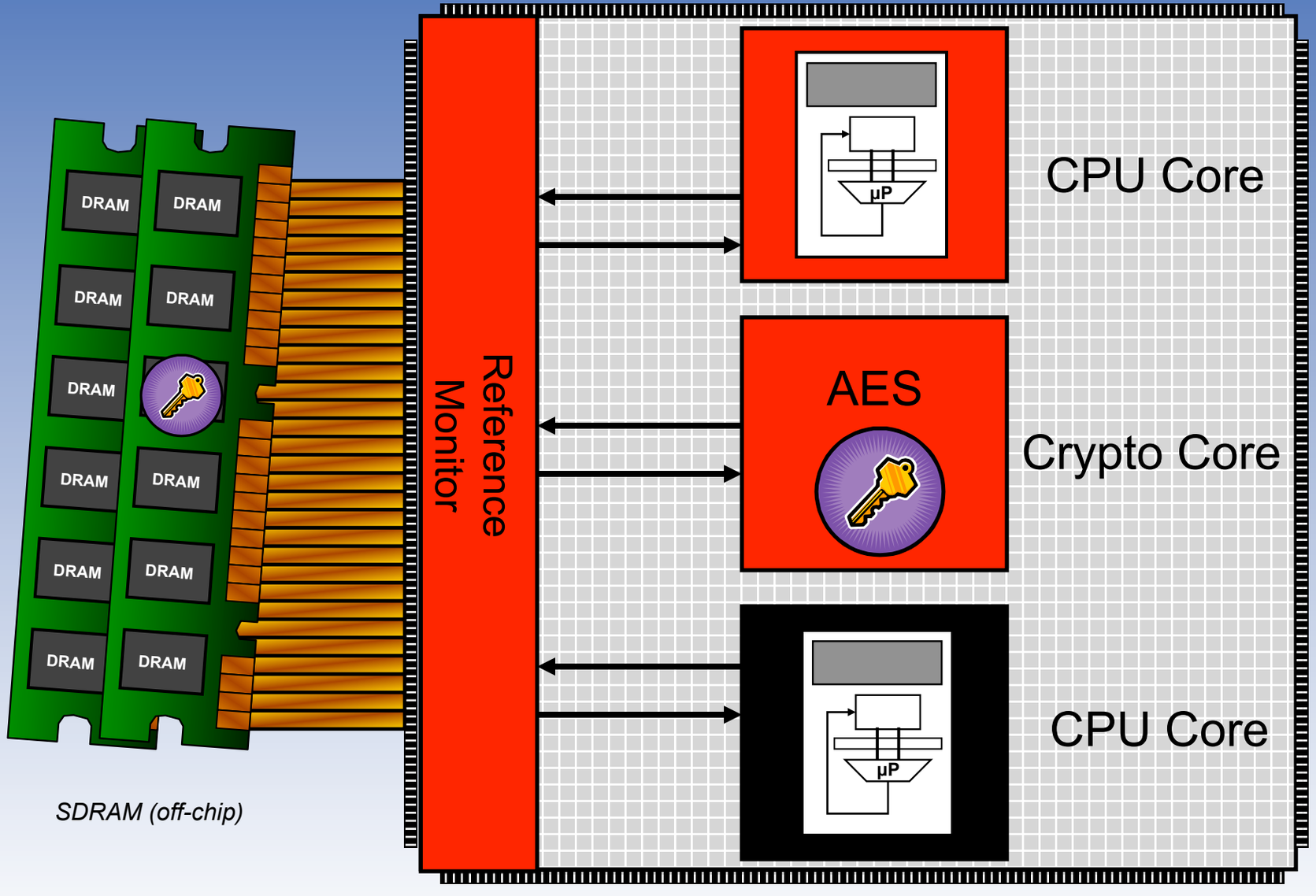
Threats and Challenges in FPGA Security

Ted Huffmire
Naval Postgraduate School
December 10, 2008

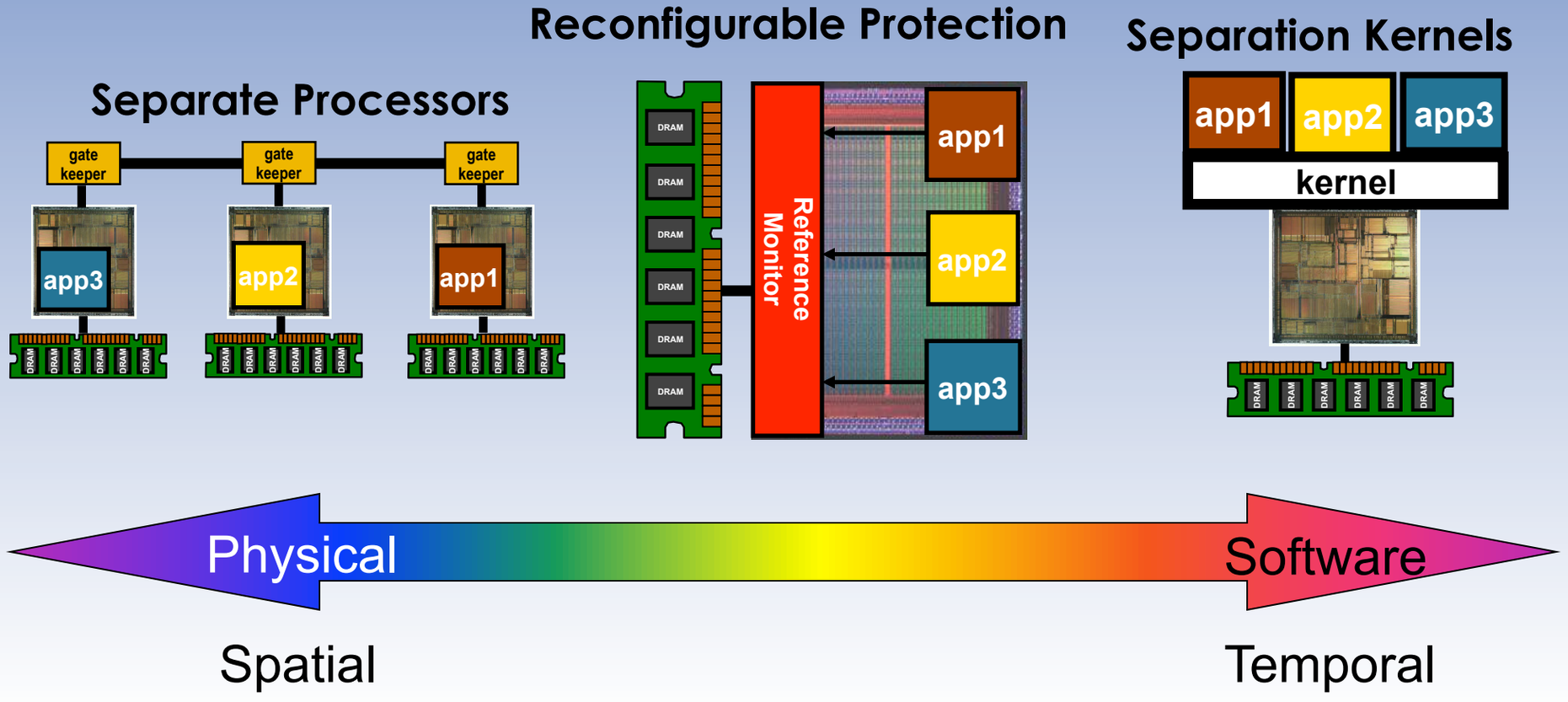
Overview

Problem Areas				
Foundry Trust	Physical Attacks	Design Tools	Design Theft	System Assurance
Attacks				
Trojan horse Backdoor Kill switch	Probing Sand and Scan Side Channels Data Remanence	Covert channels Side channels Bypass	Cloning Reverse engineer Readback attack	DoS Authentication Complex designs
Solutions				
Trusted foundries FPGAs X-Ray Inspection Sand and Scan	Tamper sensing Adding noise Degaussing	Logical isolation Tracing wires Sanitization	Continuous power Encrypt bitstream Watermarking Authentication	Reference monitor Defense in depth User training Security usability
Future Research				
All of supply chain Lessons from S/W	Red teams Side channels	Trusted tools Verification Languages CM	High-assurance Partial reconfig PUFs	High-assurance CMPs Tagging Dynamic security

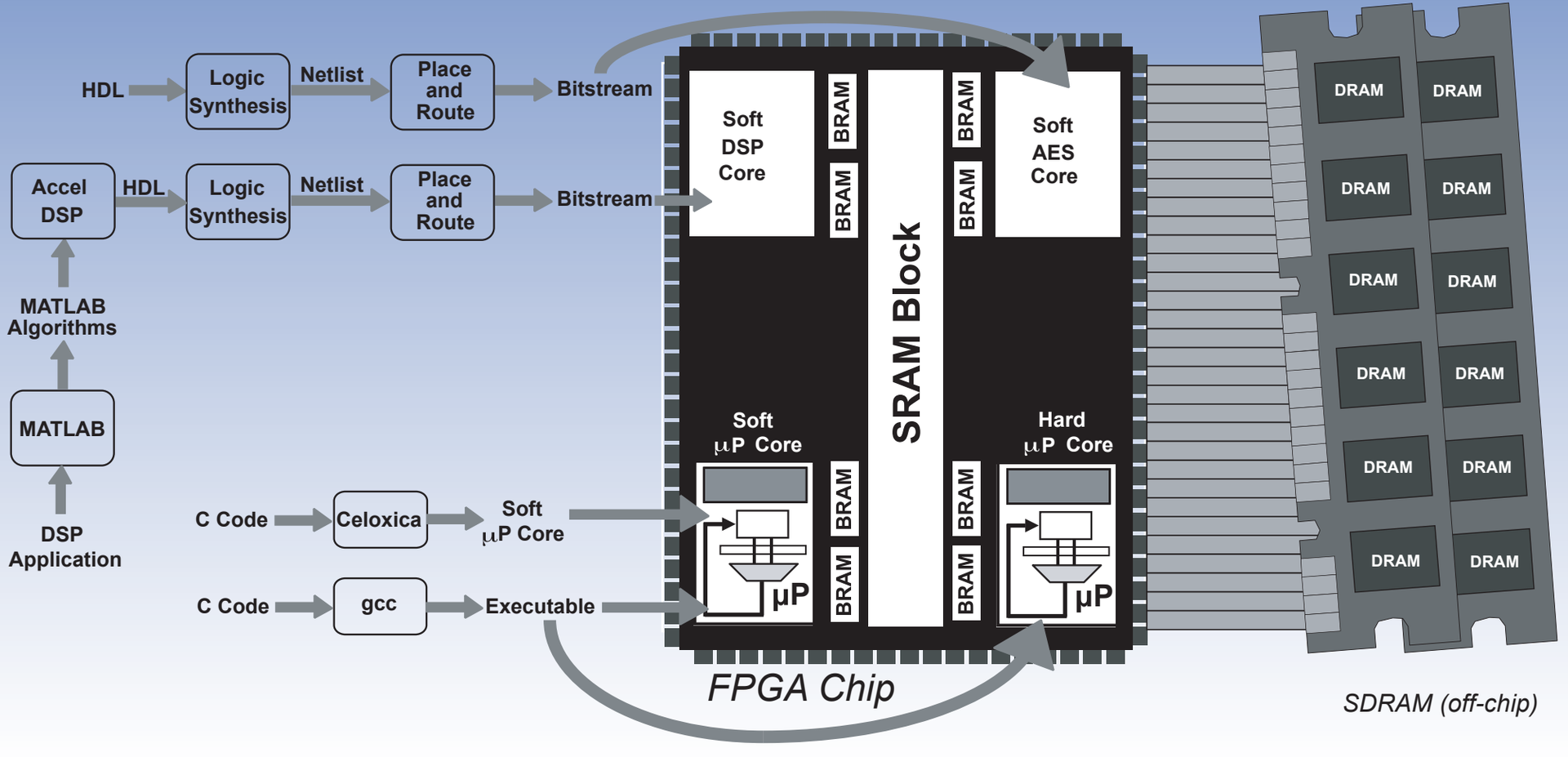
Reconfigurable Hardware



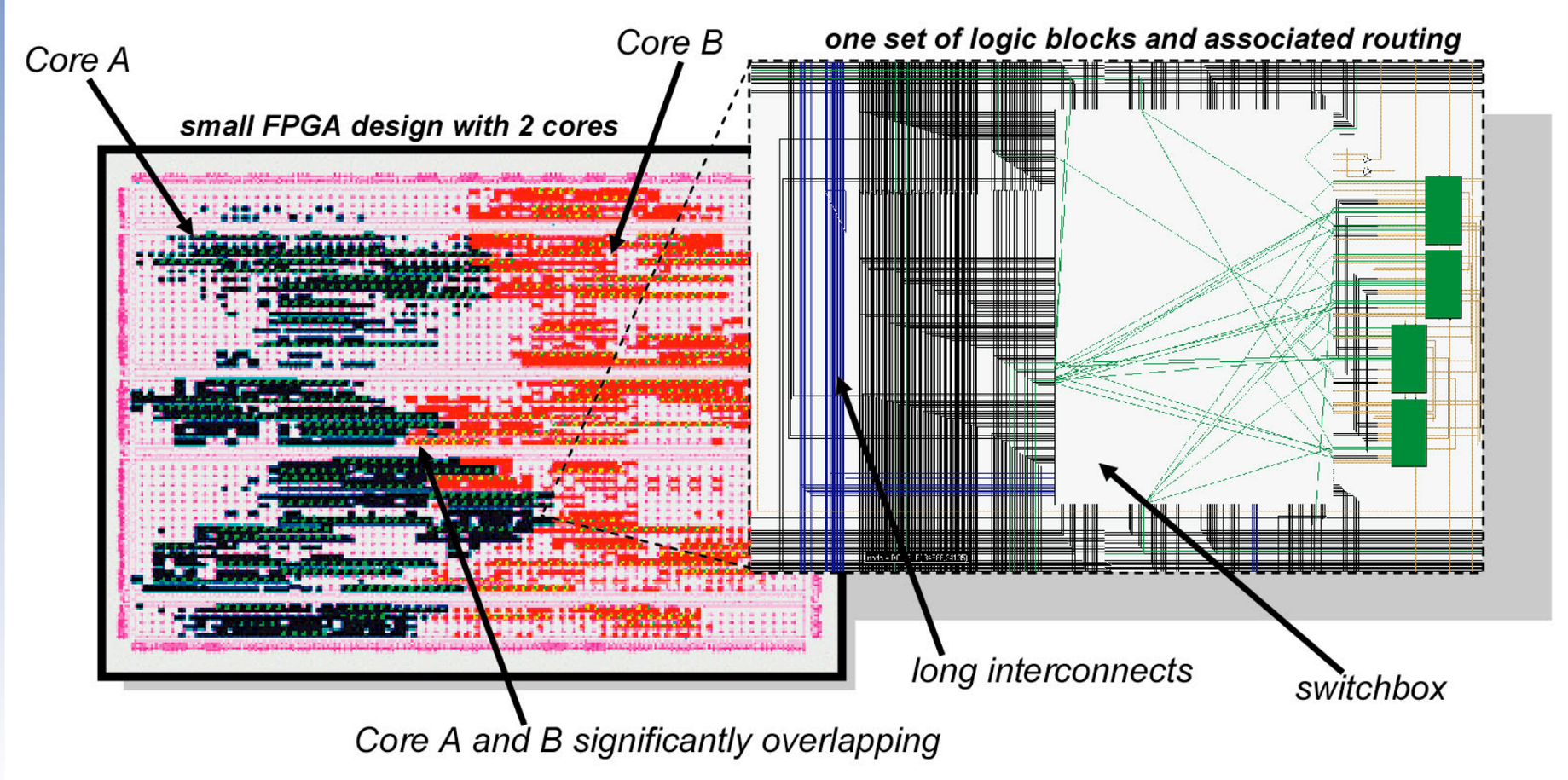
Protection Alternatives



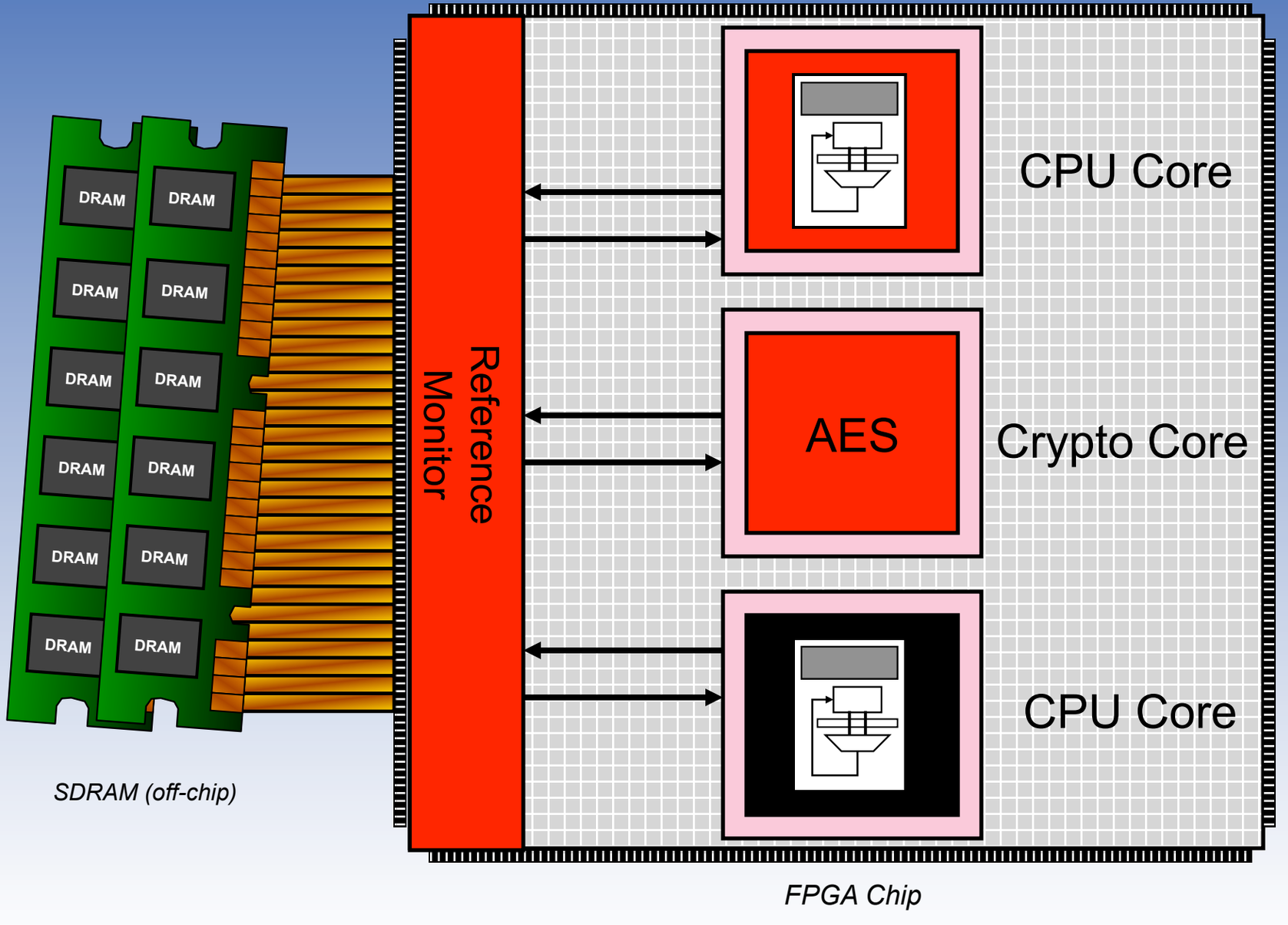
Design Flows



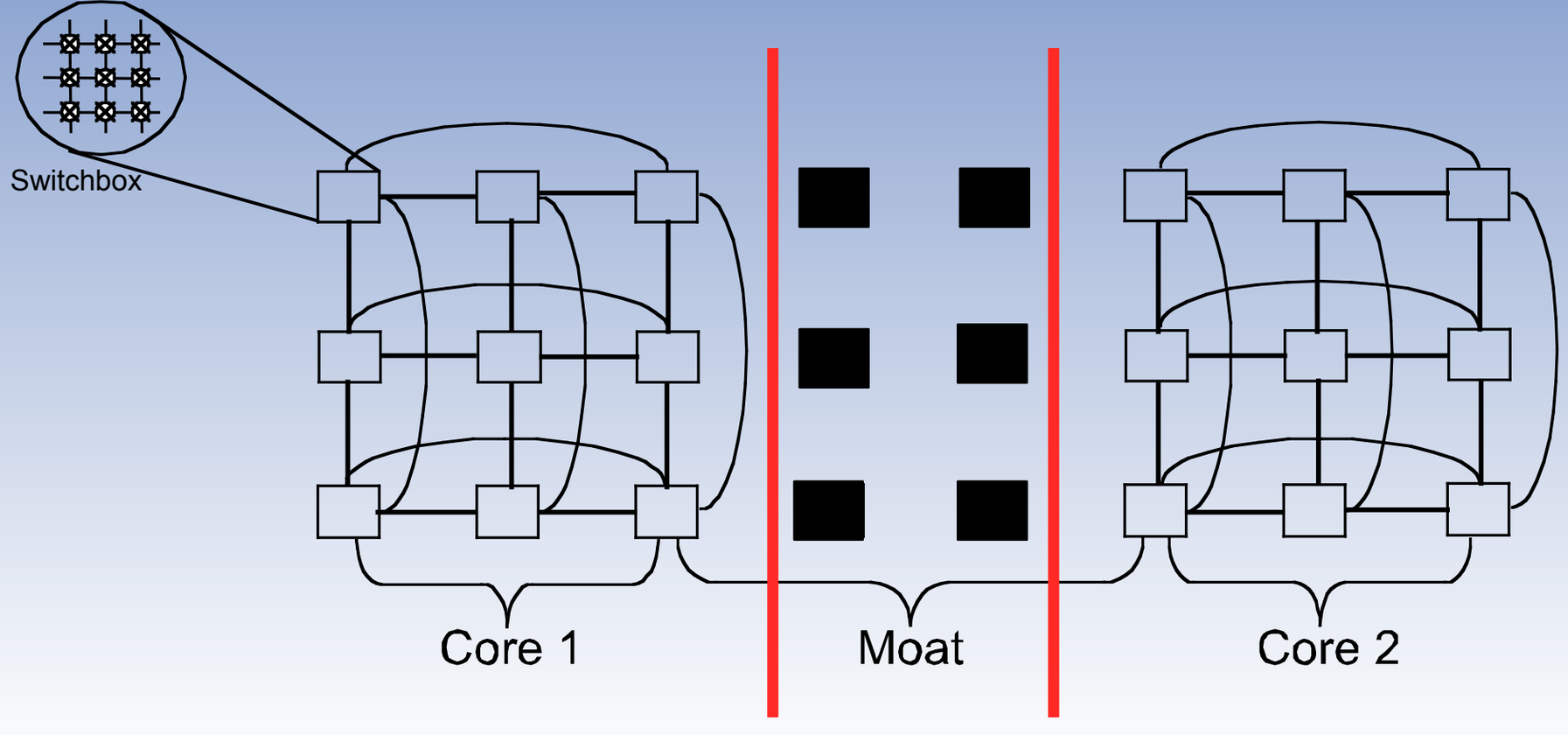
Intertwined Cores



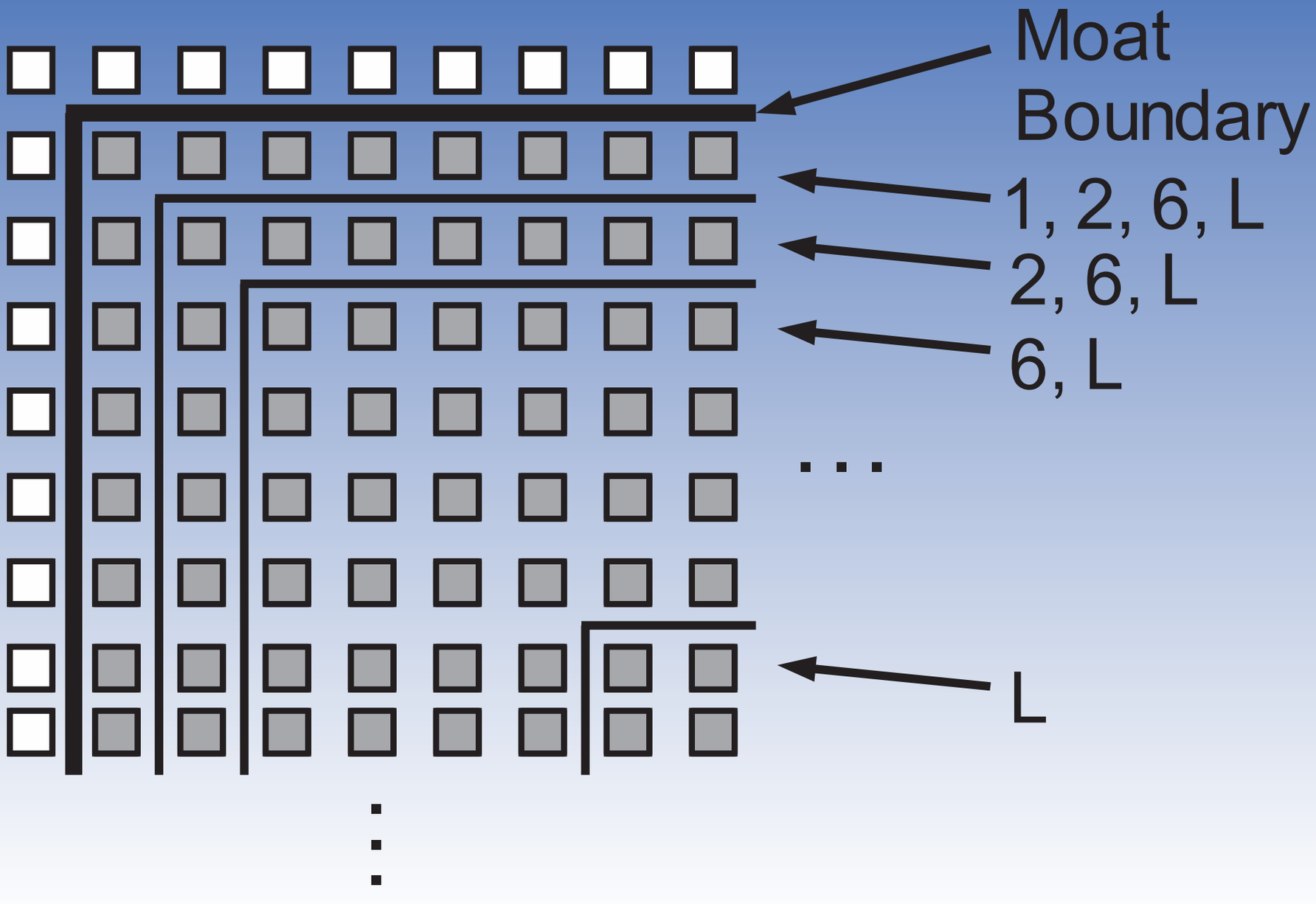
Moats


DRAM
Reference Monitor
CPU Core
AES
Crypto Core
CPU Core
SDRAM (off-chip)
FPGA Chip

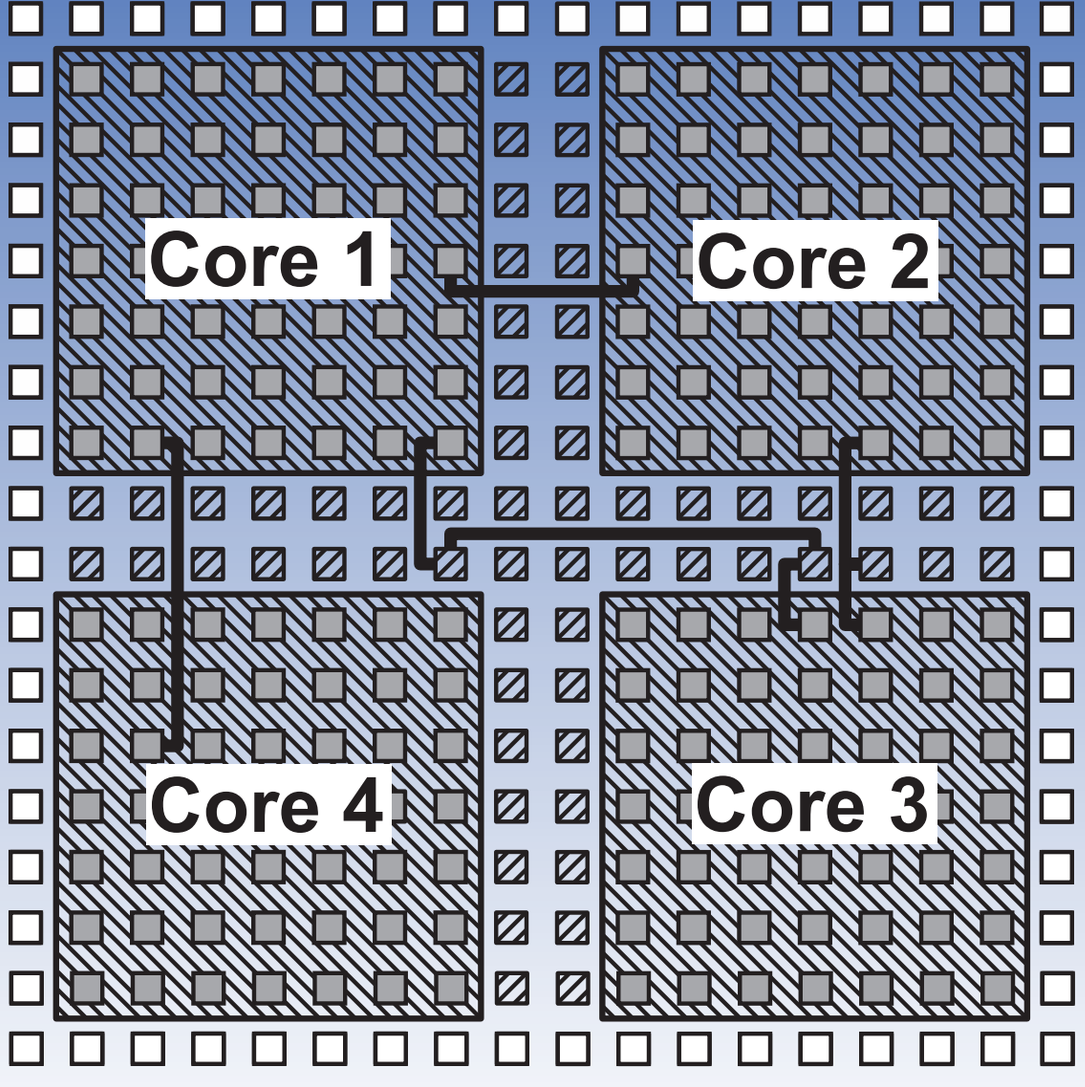
Moats 1.0



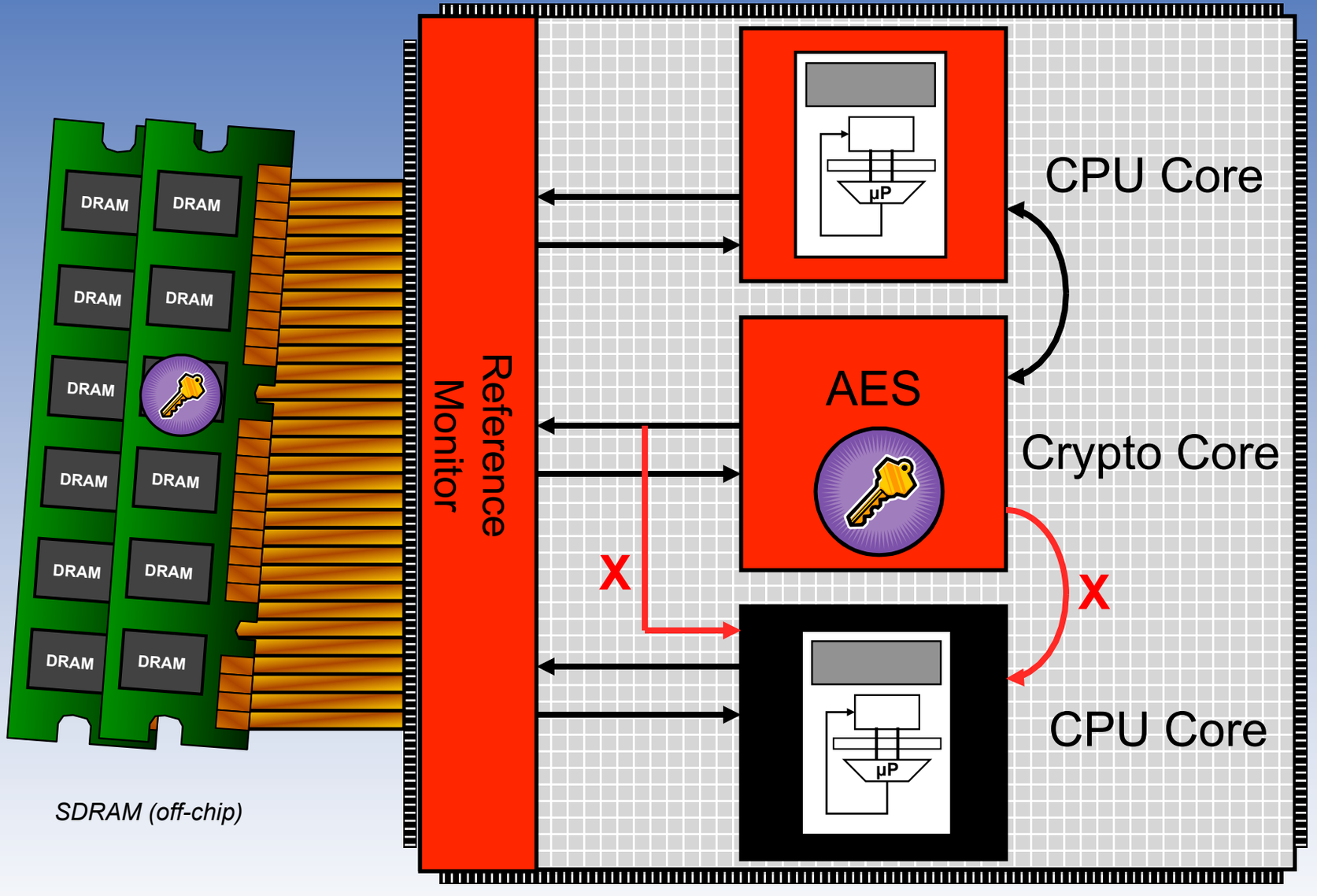
Moats 2.0



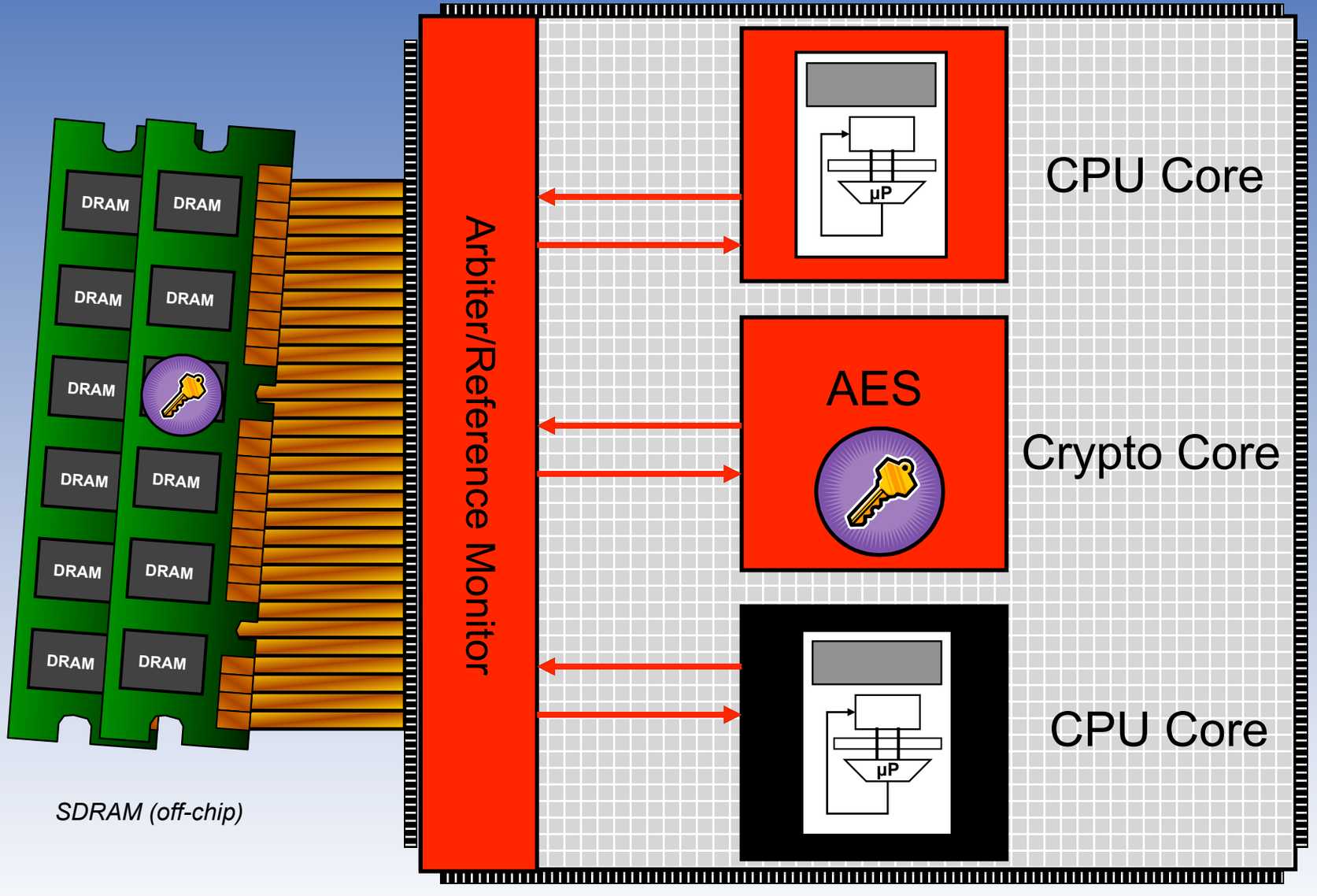
Moats and Drawbridges



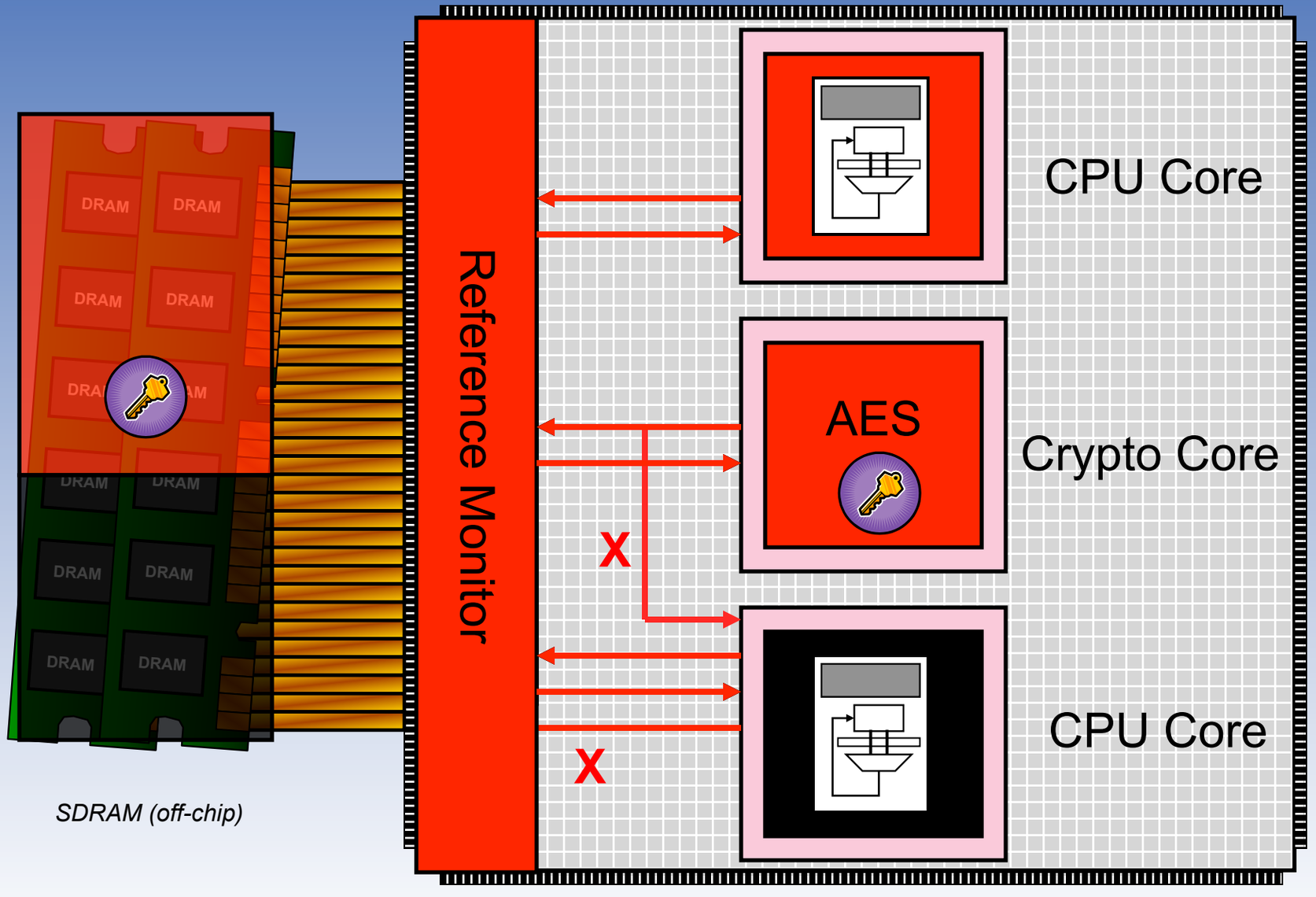
Interconnect Tracing



Communication Architecture



Memory Protection

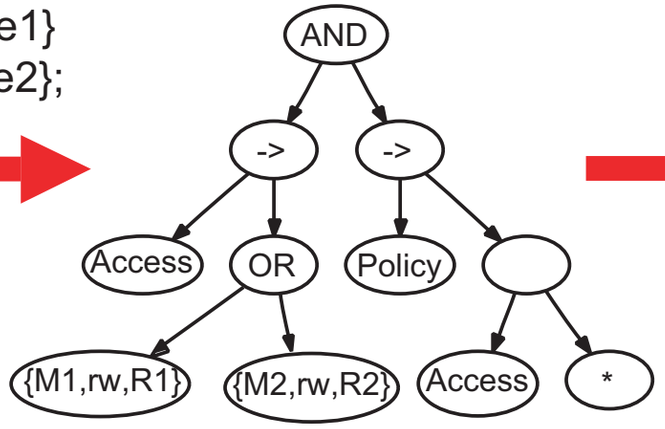


Policy Compiler

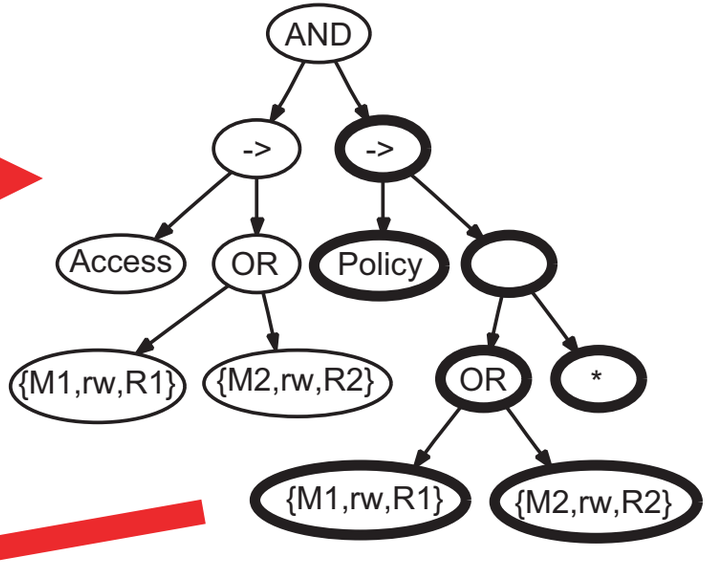
1. Policy

```
Access->{Module1,rw,Range1}
        | {Module2,rw,Range2};
Policy->(Access)*;
```

2. Build Parse Tree



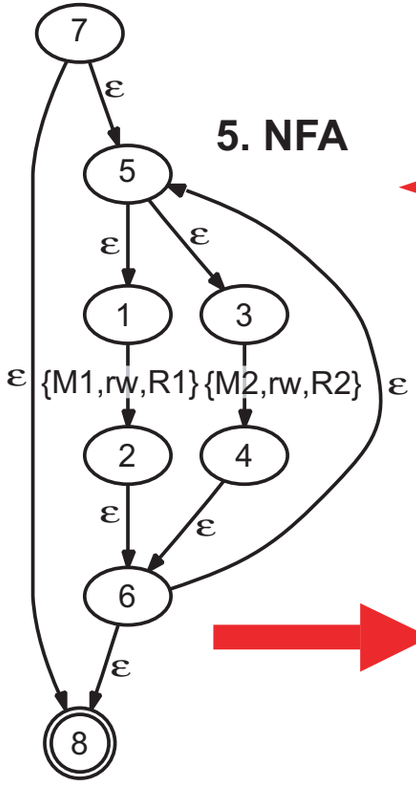
3. Transform Parse Tree



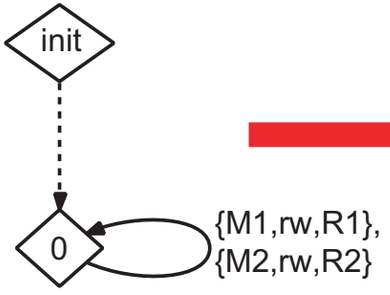
4. Regular Expression

({Module1,rw,Range1}
| {Module2,rw,Range2})*

5. NFA



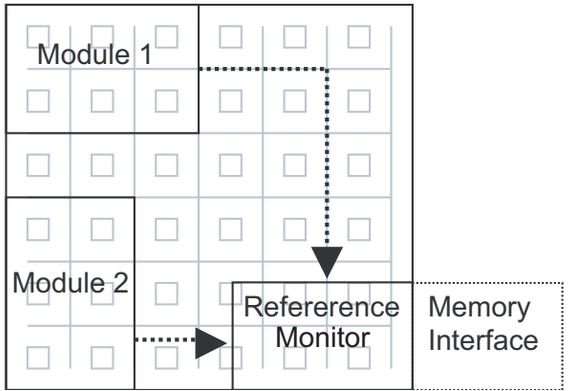
6. DFA



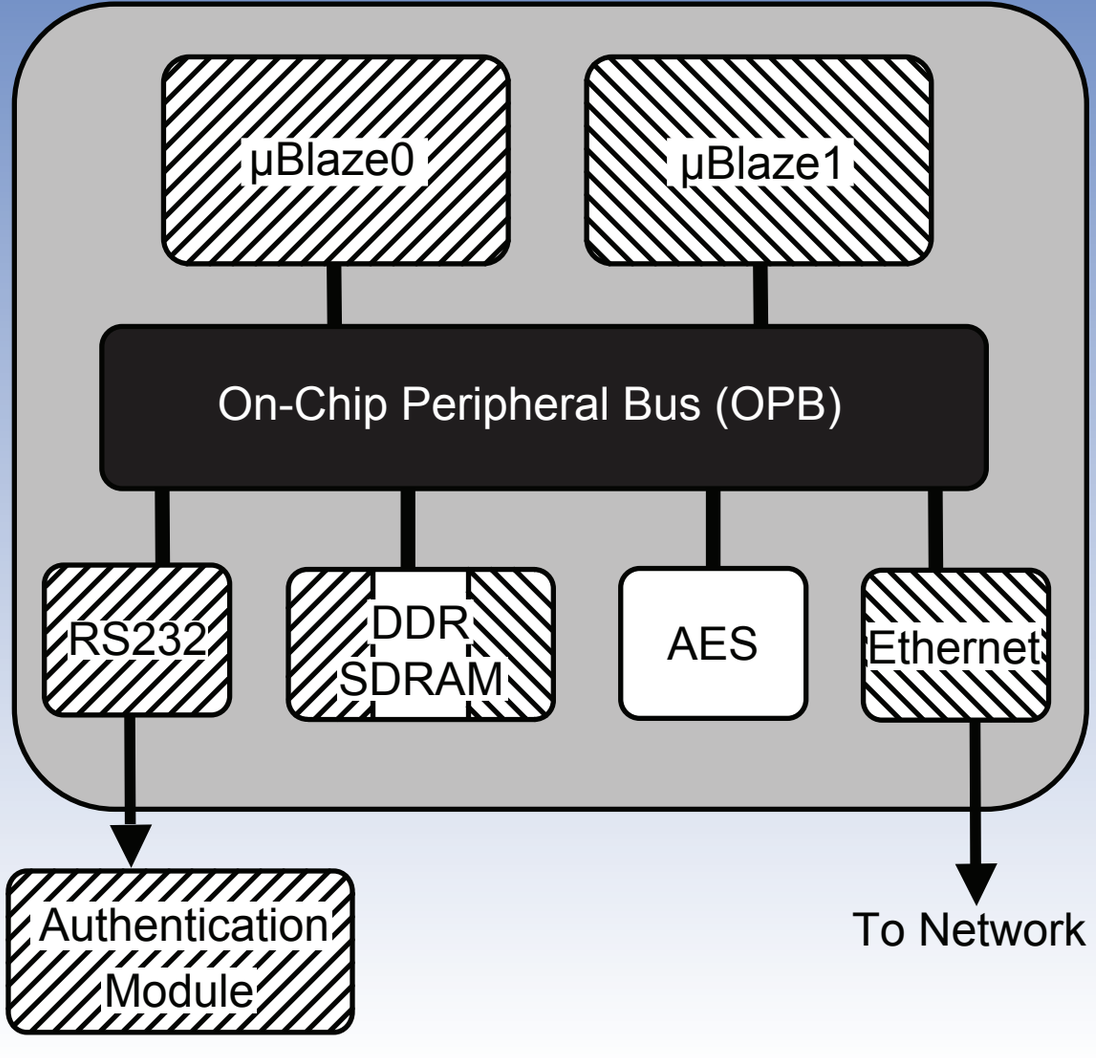
7. Verilog

```
case({module_id,op,r1,r2})
  9'b000011110: //M1,rw,R1
     state = s0;
  9'b000101101: //M2,rw,R2
     state = s0;
  default:
     state = s1; // reject
endcase
```

8. Reference Monitor



SoC Application



FPGA SUMMIT

Questions?

- http://faculty.nps.edu/tdhuffmi